

July 12, 2011

Clerks and Justices
Federal District Court
280 South First Street
San Jose CA 95113

RECEIVED

JUL 16 2011

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

Re: Public Internet Court Records Chill My Right to Petition

Dear Clerks and Court:

I have a problem with the court records being copied to the Internet and dockets exported to search engines via third party web sites. The fact that a case will be easily looked up long after the issue has passed would make me think long and hard about the permanent public exposure. **There may be incredible injustices that I would not want remedied because the quick public access to records, especially online, would be so damaging.** I was a computer software engineer and many managers and employees would search for my unique name before interviewing me and the results serve as my portfolio. In our legal system it is basically impossible to stop information from being repeated on the Internet per 47 USC § 230 which modifies the common law online. I have tried publishing my ideas and work more but often undesirable information reaches the top of the search results first.

I made a huge blunder while suffering from a "mental health moment" of a couple months where I filed suit against 7 billion John Doe defendants in C 11-00236 in the Northern California Federal District Court. Some journalist ran into this and blogged about it online and my friends found this when they went looking for me recently, providing them with substantial comical relief. The author falsely claimed I lost the case and had no understanding of the court procedures. I also consider this to be a violation of my publicity rights, something that are often impossible to secure online per 47 USC § 230 being extended so broadly. Incidents like this should be quietly ignored and not recorded because they cast someone in my situation in a bad light forever with no benefit to society. I can be medically treated extremely effectively.

My medical privacy rights were horribly violated in C 09-02324 RMW by the defendant El Camino Hospital which probably should have sealed the documents even just to admit I was ever there. I was not aware at all to the extent which the case would be publicized online, and my initial consent to publicly disclose my objection to being held involuntarily with anxiety is no longer valid because an attorney attempted to use the fact against me in a car accident case. The 47 USC § 230 case law immunizes third party sites from repeating the information from the case file online, or individuals doing so online, even after it is sealed. *I would appreciate if we could accelerate the archiving of this case. I do appreciate my motion to seal being heard early although I am confused as to why.*

It was also widely reported on that my hobby eBay rock and gem business was destroyed despite approximately one thousand successful transactions by the 47 USC § 230 law and another user when the site refused to comply with requests from both parties to remove a feedback comment, refused to accept a third-party minute order from Small Claims Court, and then finally complied when it was brought to the Superior Court where it was dismissed per 47 USC § 230. **Currently it is impossible to even obtain a court order in most incidents because the site actually holding the information can't be named as a party** with the common law crippled as it is. A larger example is Tiffany & Co. which can't keep fake jewelry (largely being sold from China) off the site even with a trademark infringement claim.

The legal solution to the information mess on the Internet could be some sort of arbitration available to parties who need unlawful content distribution stopped online. The idea would be that 47 USC § 230 is

repealed and in its place is qualified immunity to sites that cooperate with the arbitration. If they comply with requests to identify posters of user generated content, and comply with preliminary and "permanent" requests to remove content determined to be unlawful, they couldn't be sued over the third-party posting. The categories of unlawful content would include invasions of privacy, defamation, intellectual property, and classified government information. This could be a commercial service where the decisions are made on their face by a call center staff and could also be a somewhat automated process. Usually simply removing unlawful content would be satisfactory and collecting damages would be reserved for major incidents and the court system. There would be an appeal (basically a second opinion) and it would not preempt court action against the original poster even if employed because only the web site hosting the content is immunized. It could take less than a couple days.

Private web sites are not venues for free speech by third parties. The owners have the right to decide what they distribute and the public has the right to remedy unlawful damaging content. Also free speech is much more about securing the right to create civil unrest towards the government than the right to slander a private person or business. The most popular web sites promote themselves as open venues for publishing and exchange but have no good solution for the users who don't do that responsibly. A solution that provides recourse and remedy against abuse but protects free speech is desirable.

With the rapid growth of social media and Web 2.0 (as well as WikiLeaks and the exposures by the recent wave of malicious hacker attacks) some ability to quickly control unlawful damaging information is needed. Currently it takes a millionth of a cent worth of electricity to post something online that could require years and tens of thousands of dollars on average to correct in addition to the money lost. The balance is simply off in this aspect of the law.

Sincerely,

Kiel J Sturm
Engineer

An Example of My Published Work

I can't get this promoted above the flood of infringement on my publicity rights online, which also damage me and make it undesirable to be ambitious about ideas like this. I am not a public figure and I do not like be skewed in this way.

The inability to remedy defamation, invasions of privacy and publicity rights, and the lack of a good solution that also protects free speech is damaging to society and our economy.

Distributed Opt-In Email System Overview

Copyright © 2011 Kiel J Sturm

Introduction

The Distributed Opt-In Email System is an authenticated email system that employs concepts from social networking and public key encryption to create a spam and spoof-resistant secure email system. We don't need to see your face, we just want your (cryptographic) signature. Your email server (or webmail provider) helps you manage your contacts which serves as a whitelist for incoming email. The identity is enforced with public key encryption signatures on every email. This is an improvement over the spam filter concept because no spam would be accepted, mailing lists could be opted-out of effectively, and no valid emails would get lost in the filter.

Public Key Cryptography for Email

Systems such as PGP (Pretty Good Privacy), a 1992 invention now owned by Symantec, employ public key cryptography and other cryptographic technologies to authenticate the sender and thwart wiretap attempts. However they are not in widespread use in either webmail or desktop email systems. The message format is also old-fashioned plain text.

The basic features are: cryptographic signatures showing the sender is authentic, and in-transit encryption so only the intended recipients can open the email. The public key encryption system uses both a "public" key and a "private" key that work in concert. In the distributed opt-in email system your public key is stored on your email gateway so that it can be accessed by any destination email gateway to check the signature on your incoming message. If the signature on the incoming message did not come from the claimed sender, the message is rejected so spoof attempts are eliminated also.

A user can sign an email with their private key so that it is identified to the recipient as genuine, or users can encrypt the email with a public key so only the private key holder can open it. The public/private key pair is generated by the email client or webmail service and only the public key is sent to the mail gateway. In this system we employ the message signing concept only, leaving message encryption as a possible extension.

Using the Social Networking Concept for Opt-In Email

Most people use Facebook to keep track of friends and family, but many use it as an email system because they can keep their contacts centralized and avoid spam and other security issues. The distributed opt-in email system is suitable for friend, family, customer/provider and professional contacts because they can all be managed separately through your local mail server, and located through a centralized listing service called SIGBOOK. People and businesses would opt to list themselves on this site in a Yahoo!-style directory and Facebook-style social networking site.

If users choose to share their contact list with SIGBOOK (where it does not become public) then a sense of authenticity is provided by the number of contacts a person has, and the number of mutual contacts. For example Citibank would be easily recognized by having millions of contacts, and someone from your high school might have several mutual contacts. Each time you add a new contact you opt-in to receive email from them, and they would be sent a notification asking them to add you.

Businesses could group individual employee email addresses under a heading, or hide them from public listing, and promote their mailing lists and general correspondence addresses instead. Businesses could also be optionally verified with a fee service to authenticate a whole domain and display an appropriate badge. Individuals could be verified as real people using a similar service.

Modern Message Format

The distributed opt-in email system uses an XML-based email message format and a web service-based exchange protocol. This is an improvement over the plain text format email system still in use since 1982. Attachments can also be optionally directed to a file hosting service to save bandwidth and increase allowable size. The email could contain plaintext or an essential subset of HTML that just provides formatting tags.

Each message includes a signature block that is the cryptographic hash of the email encrypted with the private key. This makes the message tamper-resistant and authenticates the sender preventing spoofing attempts. The email clients check these signatures at the arrival point, or the destination email system does during message acceptance.

Web Service Enabled

The transport mechanism for messages and keys is an HTTP web service, with an SMTP migration that allows new adopters to reach users on the old email system as a fallback. To deliver the message, a sender's email application simply sends a POST request to a relay or destination email server. The exchange for a given domain would simply use the HTTP port on the domain's MX record hosts. This simplifies firewall compatibility and software implementations.

Email gateway servers would be configured to verify message senders and integrity at each acceptance, respond to public key retrieval requests, and manage contacts and incoming contact add requests, and supply a web-based user interface for email accounts to be configured. Local webmail could also be easily provided and the same gateway could serve desktop and mobile email clients.

Keep Your Email Address

The distributed opt-in email system implements a next-generation email system with the same email address format, but the system runs separately from existing email. This makes it possible to keep existing email addresses and for senders to attempt transmission with the new system before reverting to the old one. Early adopters could refuse to accept email the old way and provide a bounce message with a link to a contact form.

Retrieval from Local Mail Server

Once mail reaches your local mail server, your new client can browse an incoming mail web HTTP service and download mail messages locally to the client. Since a web application is already running for key and contact management, webmail could be provided locally also. Configuration is nearly automatic because the MX record host can be used for incoming and outgoing email, so a simple DNS lookup is all that is needed to configure a client.

Nexus

The nexus front-end sigbook.com web site would be operated by a new company and be the primary

collection of email addresses that have adopted the new system. Use of the nexus would also be optional, and organizations could provide their own internal contact collections that integrate less openly. The central site would list people in a directory, with businesses purchasing preferred listings if they want more exposure. The new company would generate revenue with these listings, traditional advertising, and identity verification features.

The nexus directory could also be accessed through a user's local mail system which would access web services at the nexus site. Users can also manually add contacts to their whitelist.

Email Gateway Software

The new email nexus company would also develop the email gateway software that it interoperates with (in a distributed way). This software would be open source because of the sometimes major and proprietary customizations organizations would need, written in Java and run in a Java application server, and come with paid customization and support contracts for organizations that need them.

The components of the software are:

- Web service for public key retrieval
- Message acceptance service to deliver messages to
- Contact manager for users that integrates with the nexus site
- An optional webmail component with per-user pricing